ADON: Anomaly Detection on the Cloud and the Internet of Things

E.G.M. Petrakis, S. Sotiriadis, N. Bessis, R. Buyya, V. Cristea, F. Pop, A. Provetti and M. Trovati

Anomalies are detected in systems as a result of malicious behavior of users or as unscheduled changes in the operation of a system. With the advent of cloud, similar behavior is now detected in virtualized environments such as the environment of a cloud provider (now affecting the operation of the system in scale and of a much large number of users) with certain economic and operational impact. Although cloud systems are considered to be more efficient, for example in terms of reliability, security etc. compared to legacy systems operating within the premises of a company, they are exposed to a much larger number of users and the internet.

At the same time, due to its scalability and affordability, the cloud is considered to be the ideal environment for deploying IoT applications. This exposes the cloud to even more risks as IoT is operating in the periphery of the cloud and is generally less protected than the cloud itself. In particular, the advent of the cloud and Internet of Things (IoT) open-up new possibilities in the design and development of methodologies ensuring reliable security protection and, in the case this fails, of methodologies for detecting and for dealing with the cause and point of system failure.

Malicious behaviour detection

Anomaly detection for malicious behavior detection which is typically expressed as (a) Fraud detection in which case, authorized of unauthorized users operate the system for the purpose of unfair or unlawful gain and (b) Intrusion detection in which case, unauthorized users are attempting to disrupt normal system operation.

Large scale system failures

Anomaly detection on large scale system failures which is due to heavy (CPU, network and memory) workloads or faulty/misconfigured resources. A special case of system failure is encountered when parts of the system fails to operate as scheduled due to power failure or material fatigue (e.g. disk failure).

IoT systems

Anomaly detection on large scale system failures which is due to heavy (CPU, network and memory) workloads or faulty/misconfigured resources. A special case of system failure is encountered when parts of the system fails to operate as scheduled due to power failure or material fatigue (e.g. disk failure).

Anomaly detection has been studied extensively in recent years and new methods are now becoming available on the cloud. Depending on application, anomalies can be detected either in real time i.e. typically by the analysis of stream data acquired by the application and operation of the system or, in batch (i.e. by analyzing system log data). Methods and systems for stream processing for example Storm, Spark, Flink, big data analysis techniques (as log data eventually become big) combined with Machine Learning techniques (for adapting anomaly detection to the peculiarities of the data and of the operation environment) are of particular importance to the design of anomaly detection methods. Combined with methods of system security analysis in virtualized environments (such as the cloud), the new era of methods for anomaly detection will soon arise.

The purpose of this Workshop in to bring together experts from the fields of distributed computing systems including security, cloud and Internet of Things as well as experts on algorithms for signal processing, log analysis, pattern recognition and statistical learning models, working in all aspects of anomaly detection such as those referred to above.